МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет управління фінансами та бізнесу
Кафедра цифрової економіки та бізнес-аналітики

ЗАТВЕРДЖЕНО
На засіданні кафедри цифрової економіки та бізнес-аналітики
факультету управління фінансами та бізнесу
Львівського національного університету
імені Івана Франка
(протокол № 1 від 28 серпня 2023 р.)

Завідувач кафедри_____І.Б. Шевчук

Силабус з навчальної дисципліни «Кіберпростір та протидія кіберзлочинності», що викладається в межах ОПП «Інформаційні технології в бізнесі» другого (магістерського) рівня вищої освіти для здобувачів з спеціальностей 051 «Економіка»

Львів 2023 р.

	Силабус навчальної дисципліни **«Кіберпростір та протидія кіберзлочинності»** **Галузь знань: 05 «Соціальні та поведінкові науки»** **Спеціальність: 051 «Економіка» та**
Адреса викладання дисципліни	м. Львів, вул. Коперника, 3
Факультет та кафедра, за якою закріплена дисципліна	Факультет управління фінансами та бізнесу Кафедра цифрової економіки та бізнес-аналітики
Галузі знань, шифри та назви спеціальності	05 «Соціальна та поведінкові науки» 051 «Економіка»
Викладачі дисципліни	Ярема Олег Романович, к.е.н., доцент кафедри цифрової економіки та бізнес-аналітики
Контактна інформація викладачів	Моб. телефон: +38(097)-545-70-16 Електронна скринька: oleh.yarema@lnu.edu.ua Telegram: https://t.me/Yarema_OR, 097-545-70-16 Сторінка викладача: https://financial.lnu.edu.ua/employee/yarema-o-r Місце знаходження: м. Львів, вул. Коперника, 3; кім. 508 (кафедра цифрової економіки та бізнес-аналітики)
Консультації з питань навчання по дисципліні відбуваються	Щовівторка, 13:30-15:00 год. (MS Teams) Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю). Можливі он-лайн консультації через Telegram. Для погодження часу он-лайн консультацій слід писати на електронну пошту викладача, писати в телеграм або дзвонити.
Сторінка курсу	https://financial.lnu.edu.ua/course/kiberprostir-ta-protydiia-kiberzlochynnosti Платформа MOODLE: https://e-learning.lnu.edu.ua/course/view.php?id=5761
Інформація про дисципліну	Дисципліна "Кіберпростір та протидія кіберзлочинності" є важливим компонентом сучасної освіти, оскільки кіберпростір став неодмінною складовою нашого повсякденного життя, а віртуальні загрози стали серйозними проблемами для суспільства. Актуальність дисципліни "Кіберпростір та протидія кіберзлочинності" у сучасному світі вкрай висока з численними обґрунтованими причинами: • Зростання кіберзлочинності • Зростання важливості інформації • Завдання державної та глобальної безпеки • Запит на професійних фахівців у галузі кібербезпеки • Широкий спектр загроз • Законодавчі та регуляторні вимоги • Розвиток технологій Зважаючи на ці фактори, дисципліна "Кіберпростір та протидія кіберзлочинності" стає критично важливою для

	підготовки кваліфікованих фахівців, які можуть захищати інформацію, інфраструктуру та безпеку в цифровому світі.
Коротка анотація дисципліни	Дисципліна “ Кіберпростір та протидія кіберзлочинності ” є нормативною дисципліною зі спеціальності 051 «Економіка» для освітньої програми «Інформаційні технології в бізнесі», яка викладається в XI семестрі в обсязі 90 годин та 3 кредитів (ECTS).
Мета та цілі дисципліни	Мета дисципліни "Кіберпростір та протидія кіберзлочинності" полягає в наданні студентам глибокого розуміння кіберпростору та кіберзлочинності, а також розвитку навичок і компетенцій, необхідних для ефективного захисту інформації, інфраструктури та безпеки в цифровому середовищі. Вивчення навчальної дисципліни “Кіберпростір та протидія кіберзлочинності” передбачає досягнення такого кваліфікаційного рівня підготовки магістра, за якого він повинен отримати: **а) знання** • Основ інформатики: Студенти повинні мати базове розуміння комп'ютерних систем, операційних систем, мереж, програмування та інших аспектів інформатики. • Основ кібербезпеки: Розуміння основних термінів і концепцій у галузі кібербезпеки, таких як аутентифікація, авторизація, шифрування, загрози, інциденти та інше. • Основ мереж і інтернету: Розуміння архітектури мереж, принципів роботи Інтернету та основних мережевих протоколів. • Основ законодавства та регуляції: Розуміння основних правових та регуляторних аспектів, пов'язаних з кібербезпекою та кіберзлочинністю. **б) уміння:** • Захист інформації: Здатність розробляти та реалізувати заходи для захисту інформації від несанкціонованого доступу, витоку даних та інших загроз. • Виявлення і реагування на кіберзлочинність: Здатність виявляти потенційні кібератаки, аналізувати їх та вживати заходи для реагування на інциденти. • Етична поведінка в кіберпросторі: Дотримання етичних норм та стандартів використання кіберпростору, у тому числі пов'язаних із захистом інформації та безпекою. • Комунікаційні навички: Здатність ефективно комунікувати з іншими фахівцями, як у сфері кібербезпеки, так і в організаціях та громадськості. • Розуміння законодавства та регуляції: Здатність визначати відповідність дій та практик законодавству та регуляторним вимогам в галузі кібербезпеки. Вимоги можуть бути дуже конкретними і можуть включати знання певних програмних засобів для кібербезпеки, навички аналізу кіберзагроз, здатність розробки планів кіберзахисту тощо. Важливо, щоб студенти були готові до вивчення складних технічних та правових аспектів кібербезпеки та кіберзлочинності.
Література для вивчення дисципліни	1. Альварез Р., Стілл Дж. Кібербезпека для початківців. – Харків: Видавництво "Сміт", 2020. – 240 с.

2. Браун К. Кіберзагрози: Технологія та захист. – Львів: Світ книг, 2017. – 240 с.
3. Власко С. Защита персональных данных: чей опыт может пригодиться Украине. Европейская правда. 2018. URL: https://www.eurointegration.com.ua/ rus/experts/ 2018/01/16/ 7076152/.
4. Галак М. Кіберзлочини: Методи, суб'єкти та вимоги для доказу. – К.: Видавництво "Юрінком Інтер", 2018. – 224 с.
5. Гібсон, Д. Кібербезпека і захист від кіберзагроз. – Львів: Видавництво "Спадок", 2020. – 296 с.
6. Елущенко Н. Что такое интернет вещей? Даже ваша бабушка это поймет. AIN. 2018. URL: https://ain.ua/special/what-is-iot/.
7. Європейський Союз, Офіційний текст Регламенту GDPR. European Data Protection Board
8. Картер, Дж. Кіберзахист в корпоративному середовищі. – Харків: Видавництво "ІнфоПрос", 2019. – 320 с.
9. Кейсер Е. В. Кіберзлочинність і право: Посібник для юристів. – К.: Юрінком Інтер, 2019. – 192 с.
10. Кеннеді, Д., О'Горман, Д., та Вінні, Д. "Metasploit: The Penetration Tester's Guide."
11. Кодекс України про адміністративні правопорушення (статті 1 - 212-24): Закон від 07 груд. 1984 р. № 8073-X. Відомості Верховної Ради Української РСР. 1984. Додаток до № 51. Ст. 1122.
12. Конституція України від 28 чер. 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
13. Кримінальний кодекс України від 05 квіт. 2001 р. №2341-111. Відомості Верховної Ради України. 2001. № 25-26. Ст. 131.
14. Ландіні, М. Інформаційна безпека: Захист даних і систем. – Дніпро: Видавництво "Престиж", 2018. – 224 с.
15. Макдональд Г. Кіберзлочинність: Підручник для студентів. – Львів: Видавництво Львівської політехніки, 2017. – 312 с.
16. Маріч, А., та інші. "GDPR: Регламент про захист персональних даних."
17. Мітнік, К., та Саймонс, В. "The Art of Deception: Controlling the Human Element of Security."
18. Мюррей, Дж., Баулинг, К. Кіберзахист і кіберзлочинність: Теорія і практика. – К.: Видавництво "ІнфоДім", 2022. – 368 с.
19. Ньюман М. Історія кіберзлочинності: Від комп'ютерних вайрусів до кібервійн. – К.: Видавництво "Наукова думка", 2019. – 368с.
20. Пригула П. 5 проблем интернета вещей, которые предстоит решить. CNews. 2016. URL: https://www.cnews.ru/articles/2016-05-27_5_ problem_ intemeta_veshchej_kotorye_ predstoit_ reshit.
21. Про захист персональних даних: Закон України від 01 чер. 2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. №34. Ст. 481.

22. Сімсон Г., Сталлінгс В. Основи комп'ютерної безпеки. – Харків: Основа, 2019. – 384 с.
23. Сімсон, Г., Хакер, Е. Кіберзахист: Засоби та методи. – К.: Видавництво "Техніка", 2021. – 448 с.
24. Сміт П. Інформаційна безпека та захист даних. – Дніпро: Діалектика, 2021. – 312 с.
25. Сталлінгс В. А. Кібербезпека: Вступ до інформаційної безпеки. – К.: Навчальний центр "Ельга", 2018. – 432 с.
26. Технология «Интернет вещей»: автоматизация настоящего благодаря разработкам будущего. IT рейтинг UA. 2020. URL: https://it- rating.in.ua/ tehnologiya-intemet-veschey-avtomatizatsiya-nastoyaschego-blagodarya- razrabotkam-buduschego.
27. Хедні, К., та Вільямс, П. "Social Engineering: The Art of Human Hacking."
28. Хілько В. І. Кіберзахист: Теорія і практика. – К.: Видавництво "Логос", 2020. – 288 с.
29. Холлінс Т. Ж. Кіберзлочинність і кібербезпека: Основи, виклики та рішення. – Дніпро: Видавництво "Ліга-Прес", 2021. – 416 с.
30. Центр досліджень армії, конверсії та роззброєння. Штучний інтелект на сторожі безпеки даних: інноваційні технології та хмарні сервіси допомагають забезпечити кібербезпеку [Електронний ресурс] Режим доступу: https://cacds.org.ua/штучний-інтелект-на-сторожі-безпеки-д
31. A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things / G. Frieder, D. Puschmann, P. Barnaghi, F. Carrez. IEEE Internet of Things Journal. 2015. №2. С. 340-354. https://doi.org/ 10.1109/ ЛОТ.2015.2411227
32. A Strategic Compass for Security and Defence, EEAS, March 2022.
33. Activation of first capability developed under PESCO points to strength of cooperation in cyber defence, EDA, February 2022.
34. Antoniuk, D., DDoS attacks hit Ukrainian government websites, The Record, February 2022.
35. Attribution to Russia of malicious cyber activity against Ukraine, Australian government, February 2022.
36. Brumfield, C., Russia-linked cyber-attacks on Ukraine: A timeline, CSO, April 2022.
37. Cerulus, L., How Ukraine became a test bed for cyberweaponry, Politico, February 2019.
38. Cerulus, L., Ukraine is getting pummeled with cyber-attacks. What's the West to do?, Politico, February 2022.
39. Cimpanu, C., Hackers deface Ukrainian government websites, The Record, January 2022.
40. Cimpanu, C., Ukraine reports cyber-attack on government document management system, Zdnet, February 2021.
41. Clayton, M., Russia Hammers Ukraine With Massive Cyber-Attack, Business Insider, March 2014.

42. Corewin: сучасні тренди кібербезпеки. [Електронний ресурс] Режим доступу: https://corewin.ua/blog/cybersecurity-trends/
43. Datami: захист вашого бізнесу в інтернеті. Безпека і кібербезпека смартфонів. [Електронний ресурс] Режим доступу: https://datami.ua/bezpeka-i-kiberbezpeka-smartfoniv/
44. Deputy Secretary General stresses NATO will continue to increase Ukraine's cyber defences, NATO, January 2022.
45. EU imposes the first ever sanctions against cyber-attacks, Council of the European Union, July 2020.
46. Fendorf, K. and Miller, J., Tracking Cyber Operations and Actors in the Russia-Ukraine War, Council on Foreign Relations, March 2022.
47. Freedom House, "Freedom on the Net" Reports. Global Internet Freedom Consortium.
48. Harding, L., Ukraine hit by 'massive' cyber-attack on government websites, The Guardian, January 2022.
49. Hern, A., Ukrainian blackout caused by hackers that attacked media company, researchers say, The Guardian, January 2016.
50. Holland, Steve. and Pearson J., US, UK: Russia responsible for cyber-attack against Ukrainian banks, Reuters, February 2022.
51. Hybrid CoE continues to work to support European security and Ukraine, Hybrid CoE, March 2022.
52. Internet of Things (IoT). European Union Agency for Cybersecurity. 2018. URF: https://www.enisa.europa.eu/topics/iot-and-smart- infrastructures/iot.
53. Ishak, N., Is Russia holding back from cyberwar?, Vox, March 2022.
54. Kagubare, I., US, EU cyber investments in Ukraine pay off amid war, The Hill, March 2022.
55. Legal service: Кібербезпека бізнесу під час війни [Електронний ресурс]. Режим доступу: https://mklegalservice.com/tpost/k123zz39h1-kberbezpeka-bznesu-pd-chas-vini
56. Madiega, T., Russia's war on Ukraine: The digital dimension, EPRS, March 2022.
57. Madnick, S., What Russia's Ongoing Cyber-attacks in Ukraine Suggest About the Future of Cyber Warfare, Harvard Business Review, March 2022.
58. Menn, J., Hacking Russia was off-limits. The Ukraine war made it a free-for-all, Washington Post, May 2022.
59. Miller, M., Despite years of preparation, Ukraine's electric grid still an easy target for Russian hackers, Politico, February 2022.
60. NotPetya, CyberLaw, May 2019.
61. NotPetya, Five Facts to Know About History's Most Destructive Cyber-attack, HYPR, June 2017.
62. Offensive Security. Документація та інструкції Metasploit Framework.
63. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

	movement of such data, and repealing Directive 95/46/EC (General Da). European Parliament and of the Council. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj. 64. Resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP)), European Parliament, 1 March 2022. 65. Resolution of 11 February 2021 on the implementation of the EU Association Agreement with Ukraine (2019/2202(INI)), European Parliament, 11 February 2022. 66. Scroxton, A., Ukraine joins Nato cyber knowledge hub, Computer Weekly, March 2022. 67. Techukraine.net. 8 інструментів IDS та IPS для кращого аналізу мережі та безпеки [Електронний ресурс] Режим доступу: https://techukraine.net/8-інструментів-ids-та-ips-для-кращого-аналізу 68. Terazus: Бізнес, технології. Топ-технології, що підкорюють бізнес цього року [Електронний ресурс] Режим доступу: https://terazus.com/uk/1164-top-texnologii-scho-pidkorjujut-biznes-tsjogo-roku 69. UK assesses Russian involvement in cyber attacks on Ukraine, Foreign, Commonwealth & Development Office and National Cyber Security Centre, United Kingdom, February 2022. 70. Ukraine accuses Russian networks of new massive cyber attacks, Reuters, February 2022. 71. Ukraine power cut 'was cyber-attack', BBC, January 2017. 72. Ukraine: Timeline of Cyber-attacks on critical infrastructure and civilian objects, CyberPeace Institute, April 2022. 73. Vazquez, M., Judd D., Lyngaas S. and Cohen, Z., Biden warns business leaders to prepare for Russian cyber attacks, CNN Politics, March 2022. 74. What is a DDoS attack?, Cloud Flare. 75. Wiper Attacks, Firewalls Security Blog. 76. Wolff, J., Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine, Time, March 2022
Тривалість курсу	90 год. для спеціальності 051 «Економіка»
Обсяг курсу	24 години аудиторних занять. З них 8 годин лекцій, 16 годин лабораторних робіт занять та 66 годин самостійної роботи для студентів 6 курсу спеціальності 051 «Економіка»
Вимоги до знань і умінь	При вивченні дисципліни «Кіберпростір та протидія кіберзлочинності» здобувачі вищої освіти набувають такі компетентності (здатність): ІК1 – Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми в економічній сфері, які характеризуються комплексністю та невизначеністю умов, що передбачає застосування теорій та методів економічної науки. ЗК3 − Здатність до абстрактного мислення, аналізу та синтезу. ЗК5 − Здатність спілкуватися державною мовою як усно, так і письмово. ЗК8 − Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК9 − Здатність до адаптації та дій в новій ситуації.

	ЗК10 − Здатність бути критичним і самокритичним. СК13 − Здатність проводити економічний аналіз функціонування та розвитку суб'єктів господарювання, оцінку їх конкурентоспроможності. СК14 − Здатність поглиблено аналізувати проблеми і явища в одній або декількох професійних сферах з врахуванням економічних ризиків та можливих соціально-економічних наслідків. СК17 − Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями. Програмні результати навчання: ПР05 − Застосовувати аналітичний та методичний інструментарій для обґрунтування пропозицій та прийняття управлінських рішень різними економічними агентами (індивідуумами, домогосподарствами, підприємствами та органами державної влади). ПР06 − Використовувати професійну аргументацію для донесення інформації, ідей, проблем та способів їх вирішення до фахівців і нефахівців у сфері економічної діяльності. ПР10 − Проводити аналіз функціонування та розвитку суб'єктів господарювання, визначати функціональні сфери, розраховувати відповідні показники які характеризують результативність їх діяльності. ПР13 − Ідентифікувати джерела та розуміти методологію визначення і методи отримання соціально-економічних даних, збирати та аналізувати необхідну інформацію, розраховувати економічні та соціальні показники. ПР25 − Розуміти структуру, основні принципи діяльності та бізнес-процеси суб'єктів ІТ-індустрії.
Ключові слова	Кіберпростір, кібербезпека, захист інформації, інтернет речей, ІКТ
Формат курсу	Очний
	Проведення лекцій, лабораторних робіт та консультації для кращого розуміння тем. Викладання навчальної дисципліни передбачає поєднання традиційних форм аудиторного навчання з елементами електронного навчання, в якому використовуються спеціальні інформаційні технології, такі як комп'ютерна графіка, аудіо та відео, інтерактивні елементи, онлайн консультування і т.п.
Теми	Подано у формі Схеми курсу
Підсумковий контроль, форма	Залік в кінці семестру(письмові завдання, теоретичні питання, тести). Оцінка складається із кількості балів нарахованих за: здачу лабораторних робіт, виконання самостійних робіт та індивідуального завдання, написання підсумкового модульної роботи. Методи контролю: спостереження за навчальною діяльністю здобувачів вищої освіти, усне опитування, письмовий контроль, тестовий контроль, виконання навчальних та індивідуальних завдань.
Пререквізити	Навчальна дисципліна взаємопов'язана із такими дисциплінами як «Інформаційні та комунікаційні технології», «Інформаційні

	системи в управлінні», «Комп'ютерні мережі», «Цифрова економіка», «ІТ-Право»
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентація, лекція-бесіда, лекція-візуалізація, колаборативне навчання (форми – групові проекти, спільні розробки і т. д.), проектно-орієнтоване навчання, навчальна дискусія, мозкова атака, кейс-метод, демонстрування, самостійна робота, лабораторні роботи, метод порівняння, метод узагальнення, метод конкретизації, метод виокремлення основного, обговорення, робота над помилками,
Необхідне обладнання	Вивчення курсу не потребує використання спеціального програмного забезпечення, крім загально вживаних програм і операційних систем. Мультимедійна дошка, проектор.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • лабораторні/самостійні тощо: 40% семестрової оцінки; максимальна кількість балів – 40; • виконання індивідуального завдання: 25% семестрової оцінки; максимальна кількість балів – 25; • контрольні заміри (модулі): 35% семестрової оцінки; максимальна кількість балів – 35; Підсумкова максимальна кількість балів – 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в практичній (письмовій) роботі студента є підставою для її незарахуваннння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції і лабораторні зайняття курсу. Студенти мають інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися усіх строків визначених для виконання усіх видів робіт, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали набрані на поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням;

	списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до заліку	1. Що таке кіберпростір і які основні складові його структури? 2. Які переваги і недоліки використання кіберпростору в сучасному світі? 3. Які основні загрози безпеці в кіберпросторі? 4. Які види кіберзлочинності існують і як вони можуть впливати на суспільство? 5. Що таке хакерство і які можливі мотивації хакерів? 6. Які заходи безпеки можуть допомогти захистити комп'ютери та інформацію від кіберзлочинців? 7. Які ролі відіграють правоохоронні органи в боротьбі з кіберзлочинністю? 8. Яким чином організації можуть захищати свою мережеву безпеку? 9. Які популярні методи соціальної інженерії використовуються кіберзлочинцями? 10. Що таке фішинг та як його визнавати та уникати? 11. Які наслідки може мати кібератака на критичну інфраструктуру? 12. Які законодавчі засоби існують для боротьби з кіберзлочинністю в вашій країні? 13. Як можуть кіберзлочинці використовувати шифрування для своїх цілей, і як його можна перехопити? 14. Як важлива кібербезпека для індивідуальних користувачів в цифровому світі? 15. Як розвиток технологій може впливати на майбутню кіберзлочинність і як готуватися до цих змін? 16. Які ризики пов'язані з використанням глобальної мережі Інтернет? 17. Які види кіберзаходів існують для захисту особистих даних в Інтернеті? 18. Які міжнародні організації і ініціативи працюють над забезпеченням кібербезпеки на світовому рівні? 19. Які основні загрози і ризики пов'язані з кібербезпекою? 20. Які види кібератак ви знаєте і як вони можуть вплинути на організації? 21. Які наслідки може мати успішна кібератака для організації? 22. Які стратегії захисту від вірусів і малвару ви можете запропонувати? 23. Які принципи дії DDoS-атаки і як їх запобігти? 24. Які кроки слід вжити в разі кібератаки або витоку даних? 25. Які стандарти та законодавство визначають вимоги до кібербезпеки? 26. Що таке етичне ведення у кібербезпеці, і чому воно важливе? 27. Як ви розумієте поняття "соціальна інженерія" і як їй запобігти? 28. Які підходи до кібербезпеки існують в Україні та чому вони важливі? 29. Як можуть суспільство і громадськість сприяти кібербезпеці?

	30. Які найбільш важливі тренди і нові технології в області кібербезпеки? 31. Як визначити потреби у кібербезпеці для конкретної організації? 32. Що таке "мультифакторна аутентифікація" і чому вона важлива для безпеки? 33. Які рекомендації ви маєте щодо створення безпечних паролів? 34. Які основні кроки для створення та впровадження політики кібербезпеки в організації? 35. Які переваги та обмеження має використання шифрування для захисту інформації? 36. Що таке "резервне копіювання" і чому це важливо для кібербезпеки? 37. Які сучасні методи інцидентного реагування і відновлення після кібератаки? 38. Як розуміти поняття "цифровий фірмовий слід" і як його захистити? 39. Які виклики пов'язані з кібербезпекою в хмарному обчисленні? 40. Як можуть кіберзагрози впливати на критичну інфраструктуру, таку як енергетика та транспорт? 41. Як організації можуть підготуватися до можливих майбутніх кібератак? 42. Які основні аспекти кібербезпеки важливі для державних органів та критичної інфраструктури? 43. Яким чином кібербезпека пов'язана з правами на приватність і громадянськими свободами? 44. Що таке Індекс свободи в інтернеті і як він розраховується? 45. Які основні складові оцінки свободи в інтернеті включає Індекс свободи в інтернеті? 46. Які країни відзначаються високими показниками свободи в інтернеті, і чому? 47. Як впливає цензура в інтернеті на громадянські свободи? 48. Що таке GDPR і які права воно надає громадянам Європейського Союзу? 49. Які основні вимоги GDPR щодо обробки особистих даних? 50. Які можливі наслідки порушення GDPR для організацій? 51. Які приклади атак, пов'язаних із соціальною інженерією, ви можете навести? 52. Як захищатися від атак соціальною інженерією? 53. Які етапи включає в себе процес тестування на проникнення? 54. Які інструменти та методики використовуються під час пентесту? 55. Які основні принципи етики пентесту? 56. Які переваги мають пентестери для виявлення вразливостей в інформаційних системах? 57. Яким чином соціальна інженерія може бути використана для зламу комп'ютерних систем? 58. Які правила треба дотримувати для забезпечення конфіденційності особистих даних відповідно до GDPR? 59. Які сфери життя охоплює індекс свободи в інтернеті?

	60. Як впливає Індекс свободи в інтернеті на політику країн? 61. Які найважливіші аспекти безпеки інтернету слід враховувати в повсякденному використанні мережі? 62. Як можна захистити свою організацію від атак на проникнення? 63. Які зміни в кібербезпеці та приватності можна очікувати в майбутньому? 64. Що таке кібербезпека і чому вона важлива для сучасного суспільства? 65. Які основні загрози кібербезпеці існують сьогодні? 66. Які конкретні технології впливають на кібербезпеку бізнесу? 67. Як штучний інтелект впливає на конфіденційність і безпеку даних? 68. Які можливості пропонує генеративний штучний інтелект для обробки даних? 69. Як чат-боти можуть бути використані для поліпшення користувацького досвіду (CX) та досвіду співробітників (EX)? 70. Дайте приклади сценаріїв використання блокчейну в бізнесі. 71. Які виклики і можливості з'являються завдяки цифровим технологіям у сфері охорони здоров'я? 72. Чому сталі технології стають пріоритетом для компаній? 73. Що таке система виявлення вторгнень (IDS) і як вона працює? 74. Які основні функції системи запобігання вторгненням (IPS)? 75. В чому полягає важливість IDS і IPS для кібербезпеки мережі? 76. Назвіть кілька популярних програмних рішень для IDS і IPS. 77. Які основні загрози для кібербезпеки смартфонів? 78. Які заходи можна прийняти для захисту свого смартфона від кіберзагроз? 79. Як правовий аспект впливає на кібербезпеку в Інтернеті речей (IoT)? 80. Які потенційні загрози інтернету речей можуть виникнути з точки зору конфіденційності та безпеки? 81. Які законодавчі заходи вже прийняті для забезпечення кібербезпеки в сфері IoT? 82. Які основні принципи кібербезпеки, які потрібно враховувати при роботі з сучасними технологіями? 83. Як бізнес може адаптувати свої стратегії для кращого захисту від кіберзагроз і використання сучасних технологій для своєї переваги?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Викладач _____О.Р. Ярема